UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

LAUREN COPELAND and LEE WOODS, on behalf of themselves and all others similarly situated, Plaintiff, v. **STURM, RUGER & COMPANY, INC.,** and **FREESTYLE SOLUTIONS, INC.,** Defendants.	Case No.

CLASS ACTION COMPLAINT

Plaintiffs, Lauren Copeland and Lee Woods, individually and on behalf of the Classes defined below of similarly situated persons ("Plaintiffs"), allege the following against Sturm, Ruger, & Company, Inc. ("Ruger") and Freestyle Solutions, Inc., ("Freestyle" collectively "Defendants") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

INTRODUCTION

1. Plaintiffs bring this class action against Defendants for its failure to properly secure and safeguard Plaintiffs' and other similarly situated Defendants' customers' first and last names, shipping addresses, email addresses, credit and debit card numbers and expiration dates, security codes, and billing addresses, or other sensitive records from hackers.

2. Ruger is an American firearm manufacturing company based in Southport, Connecticut. The company was founded in 1949 has been publicly traded since 1969. Ruger is the largest firearms manufacturer in the United States.

3. Freestyle produces and licenses software for order processing, inventory tracking, purchasing and fulfillment for eCommerce platforms.

4. Freestyle hosted Ruger's eCommerce website ShopRuger.com. Plaintiffs purchased items such as ammunition magazines, clothing, and similar accessories from ShopRuger.com. Unbeknownst to Plaintiffs, the ShopRuger.com website was infected with malware which allowed unauthorized third parties to access their highly confidential personal information when they purchased items from the website.

5. On August 18, 2022, Ruger filed official notice of the incident with the Montana Department of Justice. Under state law, organizations must report breaches involving Social Security numbers, driver's license numbers, bank or credit card account numbers, or medical records.

6. Also on August 18, 2022, Ruger sent out data breach letters to all individuals whose information was compromised as a result of the recent data security incident, including Plaintiffs.

7. Based on the Notice Letter[1] filed by Ruger, it was notified on August 2, 2022, by Freestyle that malware had been present on the ShopRuger.com website from September 18, 2020, through February 3, 2022, (the "Data Breach"), the date the malware was removed. Neither Ruger nor Freestyle provide any explanation for the six-month delay in becoming aware of the malware and Freestyle's initial notice to Ruger.

[1] A copy of which can be viewed here: https://media.dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-504.pdf

8. As a result of this delayed response, Plaintiffs and Class Members had no idea their Private Information had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

9. Information compromised in the Data Breach included highly sensitive data that represents a gold mine for data thieves. This includes first and last name, shipping address, email address, payment card number, expiration date, security code, and billing address, (collectively the "Private Information") and additional personally identifiable information ("PII") that Ruger collected and maintained.

10. Armed with the Private Information accessed in the Data Breach, and a six-month head start, data thieves can commit a variety of crimes including, e.g., making fraudulent purchases, pilfering private email information in order to commit identity theft such as opening new financial accounts in Class Members' names.

11. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft. Plaintiffs and Class Members may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

12. In addition to the traditional financial harms that are common to data breaches of this type, Ruger is a firearms manufacturer and this data breach included information regarding the nature of each purchase. This means that the cyber criminals now have a ready, up-to-date list of homes with firearms. Guns represent a particularly attractive target for criminals, given both

their value and their use in other criminal enterprises. According to a 2017 study published in the journal "Injury Epidemiology," approximately 380,000 guns are stolen every year in this country.[2] That represents a more than 60% increase from a 2012 Department of Justice survey that found that between 2005 and 2010 on average 232,400 guns were stolen each year.[3] Given the rising prevalence of gun theft, the fact that criminals now know Plaintiffs and Class Members own guns and have a recent address for where the guns are kept, means that Plaintiffs and Class Members must take extra precautions to safeguard themselves and their firearms for years to come, and must live in fear that they will be targeted for theft simply for making a purchase on the ShopRuger.com website.

13. Therefore, Plaintiffs and Class Members will show that they have suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

14. Plaintiffs bring this class action lawsuit to address Defendants' inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and Class Members that their information had been subject to the unauthorized access and precisely what specific type of information was accessed.

15. The potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendants, and thus Defendants were on notice that failing to

---

[2] Hemenway, D., et al. *Whose guns are stolen? The epidemiology of Gun theft victims* (Inj. Epidemiol., Dec. 2017), *available at* https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5385318/

[3] Langton, L., *Firearms Stolen during Household Burglaries and Other Property Crimes, 2005–2010* (Bureau of Justice Statistics, Nov. 2012), *available at* https://bjs.ojp.gov/content/pub/pdf/fshbopc0510.pdf

take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

16. Defendants and their employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendants properly monitored the ShopRuger website, one or both of them would have discovered the breach sooner.

17. Plaintiffs' and Class Members' identities are now at risk because of Defendants' negligent conduct since the Private Information that Freestyle collected and maintained on Ruger's behalf is now likely in the hands of data thieves and unauthorized third-parties.

18. Plaintiffs seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

19. Plaintiffs seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendants' data security systems, future annual audits, and adequate credit monitoring services funded by Defendants.

PARTIES

20. Plaintiff Lee Woods, is, and at all times mentioned herein was, an individual citizen of the State of Texas residing in the City of San Antonio.

21. Plaintiff Lauren Copeland is, and at all times mentioned herein was, an individual citizen of the State of Michigan residing in the City of Harper Woods.

22. Defendant Sturm, Ruger & Company, Inc. is, and all times mentioned herein was, a firearms manufacturer with its principal place of business at 1 Lacey Place Southport, CT 06890.

23. Defendant Freestyle Solutions, Inc., is, and all times mentioned herein was, an order and inventory management software service provider with its principal place of business at 9 Campus Dr, Parsippany, NJ 07054.

JURISDICTION AND VENUE

24. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Defendants. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

25. This Court has jurisdiction over each of the Defendants because each operates in this District, and the computer systems implicated in this Data Breach are likely based in this District.

26. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District.

RUGER COLLECTS HIGHLY SENSITIVE CUSTOMER INFORMATION

27. Ruger is a firearms manufacturer founded in 1949 and based in Southport, Connecticut. It is one of the largest firearms manufacturers in the United States with more than 2,000 employees and annual revenue exceeding $650 million per year.

28. Ruger contracts with Freestyle Solutions to provide inventory and order management services for its website ShopRuger.com. ShopRuger.com sells firearms accessories such as magazines, sights, slings, and parts as well as Ruger-branded clothing and other items.

29. When purchasing an item on ShopRuger.com, customers provide:

- Names;
- Addresses;
- Citizenship Information (for some items such as magazines, barrels, and similar parts);
- Financial account information;
- Payment card information;

30. At the time of the breach, Ruger promised its customers that it would not share this Personal Information with third parties, except in limited circumstances:

> **With Whom Do We Share the Personal Information?**
> The Personal Information that we collect on our Web Sites may be shared in the following cases:
>
> **Third Parties Providing Services on Our Behalf.** We may share Personal Information with our agents and representatives who perform services on our behalf. This includes third parties that host or operate certain functions or features of one or more of the Web Sites, send communications on our behalf (including marketing e-mails), process credit card and other payment transactions, fulfill orders, analyze data, provide marketing assistance, or create, host and/or provide customer service on our behalf. These third parties may have access to Personal Information in order to provide these services to us or on our behalf, but are permitted to use such Information only in accordance with the terms of this Privacy Policy.
>
> **Sweepstakes, Contests and Promotions.** We may offer sweepstakes, contests, and other promotions (collectively, "Promotions") through the Web Sites. If you choose to participate in a Promotion, Personal Information about you may be disclosed to third parties or the public in connection with the administration of such Promotion, including, without limitation, in connection with winner selection, prize fulfillment, and as required by law or permitted by the Promotion's official rules, such as on a winners list. Also, by entering a Promotion, you are agreeing to the official rules that govern that Promotion, which may contain specific requirements of you, including, except where prohibited by law, allowing the sponsor(s) of the Promotion to use your name, voice and/or likeness in advertising or marketing associated with the promotion.
>
> **Business Transfers and Corporate Changes.** We reserve the right to disclose and transfer Personal Information: (1) to a subsequent owner, co-owner or operator of one or more of the Web Sites; or (2) in connection with a corporate merger, consolidation, or restructuring, the sale of substantially all of Sturm, Ruger's stock and/or assets, or other corporate change, including, without limitation, during the course of any due diligence process.
>
> **Legal Requirements and Law Enforcement.** We may also transfer and disclose Personal Information to third parties: (1) in the event we are required to respond to a court order, subpoena, discovery request, or other legal process, or if in our good faith opinion such disclosure is required by law; (2) at the request of governmental authorities conducting an audit or investigation; (3) to verify or enforce compliance with our Terms of Use, other agreements or policies governing a Web Site, or applicable laws, rules, and regulations; or (4) whenever we believe disclosure is necessary to limit our legal liability or to protect or enforce the rights, interests, or

> safety of a Web Site, its users or other third parties. We also reserve the right to report to law enforcement agencies any activities that we, in good faith, believe to be unlawful.
>
> Except as indicated above, Sturm, Ruger will not disclose to others any of your Personal Information unless we have your express permission.
>
> Sturm, Ruger may, however, share non-personally identifiable information, such as Web Site Usage Information or other aggregated user statistics, as well as anonymous information derived from Personal Information, such as de-identified user information, with third parties for any purpose.

31. Freestyle Solutions is Ruger's third-party software vendor that owns and manages the server hosting ShopRuger.com.

32. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendants assumed legal and equitable duties and knew or should have known, based, *inter alia*, on the prior data breach and settlement, that it was responsible for protecting Plaintiffs' and Class Members' Private Information from disclosure.

33. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

34. Plaintiffs and the Class Members relied on Defendants to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

DEFENDANTS' DATA BREACH AND NOTICE TO PLAINTIFFS

35. Plaintiffs were customers of ShopRuger.com. When customers of ShopRuger.com make a purchase on the website, Defendants collected personal and financial information, such as payment card information, along with personal information such as name, address and citizenship information.

36. According to a Data Breach Notification Letter provided to the Vermont Attorney General,[4] Freestyle notified Ruger that its software contained malware that exposed the PII of consumers on August 2, 2022.

37. Freestyle discovered this malware in February 2022 and further investigation discovered that the malware had been in place since at least September 18, 2020 through February 3, 2022, the date upon which Freestyle removed the malware from its servers.

38. Defendants waited until August 16, 2022, about 6 months after the Class's Personal Information was last accessed by cybercriminals, to finally begin to notify customers that its investigation identified that their Personal Information was breached.

39. Defendants delivered Data Breach Notification Letters (the "**Notice Letter**") to Plaintiffs and the Class Members, alerting them that their highly sensitive PII had been exposed in a data breach.

40. The Notice Letter revealed for the first time that the malware collected unencrypted data when a consumer clicked the "submission" button on the ShopRuger.com check-out page. This data included: first and last name, shipping address, email address, payment **card number, expiration date, security code**, description of the product purchased, price, and quantity.

41. The Notice Letter then attached several pages titled as a "Reference Guide" listed generic steps that victims of data security incidents can take, such as examining account statements, getting a copy of a credit report or notifying law enforcement about suspicious financial account activity.

42. On information and belief, Ruger sent a similar generic letter to all individuals affected

43. Defendants had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

---

[4] https://ago.vermont.gov/blog/2022/08/16/sturm-ruger-company-data-breach-notice-to-consumers/

44. Plaintiffs and Class Members provided their Private Information to Defendants with the reasonable expectation and mutual understanding that Ruger would comply with its obligations to keep such information confidential and secure from unauthorized access and to provide timely notice of security breaches.

RUGER FAILED TO COMPLY WITH FTC GUIDELINES

45. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making.

46. In October 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

47. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

48. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15

U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

49. On information and belief, Ruger failed to properly implement basic data security practices. Ruger's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

50. Ruger was at all times fully aware of its obligation to protect the PII of its customers.

DEFENDANTS FAILED TO COMPLY WITH INDUSTRY STANDARDS

51. Experts studying cyber security routinely identify ecommerce platforms as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

52. Several best practices have been identified that a minimum should be implemented by ecommerce providers like Defendants, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data, and; limiting which employees can access sensitive data.

53. A number of industry and national best practices have been published and should be used as a go-to resource when developing a business' cybersecurity standards. The Center for Internet Security ("CIS") released its Critical Security Controls. The CIS Benchmarks are the only consensus-based, best-practice security configuration guides both developed and accepted by government, business, industry, and academia.[5]

54. Other best cybersecurity practices that are standard in the ecommerce industry include installing appropriate malware detection software; monitoring and limiting the network

[5] *CIS Benchmarks FAQ*, Center for Internet Security, *available at* https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq (last visited August 10, 2022).

ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

55. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

FBI, FTC, NIST Guidelines on Protecting Customer Personal Information

56. Recently, the FBI issued a warning to companies about this exact type of fraud. In the FBI's Oregon FBI Tech Tuesday: Building a Digital Defense Against E-Skimming, dated October 22, 2019, the agency stated:

> This warning is specifically targeted to . . . businesses . . . that take credit card payments online. E-skimming occurs when cyber criminals inject malicious code onto a website. The bad actor may have gained access via a phishing attack targeting your employees—or through a vulnerable third-party vendor attached to your company's server.

57. The FBI gave some stern advice to companies like Defendants:

Here's what businesses and agencies can do to protect themselves:

- Update and patch all systems with the latest security software.
- Anti-virus and anti-malware need to be up-to-date and firewalls strong.
- Change default login credentials on all systems.
- Educate employees about safe cyber practices. Most importantly, do not click on links or unexpected attachments in messages.
- Segregate and segment network systems to limit how easily cyber criminals can move from one to another.

58. But Defendants apparently did not take this advice because hackers scraped customers' PII off its website—and continued to do so until at least February 3, 2022.

59. Similarly, the Federal Trade Commission ("FTC") has held that the failure to employ reasonable measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTC Act (codified by 15 U.S.C. § 45).

60. Under the FTC Act, Defendants are prohibited from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

61. Beginning in 2007, the FTC released a set of industry standards related to data security and the data security practices of businesses, called "Protecting Personal Information: A Guide for Businesses" (the "FTC Guide"). In 2011, this guidance was updated to include fundamental data security principles for businesses. In addition to the necessity to protect consumer data, the guide established that:

- Businesses should dispose of personal identifiable information that is no longer needed;
- Businesses should encrypt personal identifiable information and protected cardholder data stored on computer networks so that it is unreadable even if hackers are able to gain access to the information;
- Businesses should thoroughly understand the types of vulnerabilities on their network (of which malware on a point-of-sale system is one) and how to address said vulnerabilities;
- Businesses should implement protocols necessary to correct security breaches;
- Businesses should install intrusion detection systems to expose security breaches at the moment they occur;
- Businesses should install monitoring mechanisms to watch for massive troves of data being transmitted from their systems; and,
- Businesses should have an emergency plan prepared in response to a breach.

62. On information and belief, Defendants failed to adequately address the foregoing requirements in the FTC Guide.

63. In 2015, the FTC supplemented the FTC Guide with a publication called "Start with Security" (the "Supplemented FTC Guide"). This supplement added further requirements for businesses that maintain customer data on their networks:

- Businesses should not keep personal identifiable information and protected cardholder data stored on their networks for any period longer than what is needed for authorization;
- Businesses should use industry-tested methods for data security; and,
- Businesses should be continuously monitoring for suspicious activity on their network.

64. Again, Defendants apparently failed to adequately address these requirements enumerated in the Supplemented FTC Guide.

65. The FTC Guide is clear that businesses should, among other things: (1) protect the personal customer information they acquire; (2) properly dispose of personal information that is no longer needed; (3) encrypt information stored on computer networks; (4) understand their network's vulnerabilities; and (5) implement policies for installing vendor-approved patches to correct security vulnerabilities. The FTC guidance also recommends that businesses: (1) use an intrusion detection system to expose a breach as soon as it occurs; (2) monitor all incoming traffic for activity indicating that someone may be trying to penetrate the system; and (3) watch for large amounts of data being transmitted from the system. Plaintiffs believe that Defendants did not follow these recommendations, and as a result exposed hundreds of thousands of consumers to harm.

66. Furthermore, the FTC has issued orders against businesses for failing to employ reasonable measures to safeguard customer data. The orders provide further public guidance to businesses concerning their data security obligations.

67. Defendants knew or should have known about their obligation to comply with the FTC Act, the FTC Guide, the Supplemented FTC Guide, and many other FTC pronouncements regarding data security.

68. Thus, among other things, Defendants' misconduct violated the FTC Act and the FTC's data security pronouncements, led to the Data Breach, and resulted directly and proximately in harm to Plaintiffs and the Class Members.

69. Additionally, the National Institute of Standards and Technology (NIST) provides basic network security guidance that enumerates steps to take to avoid cybersecurity vulnerabilities. Although use of NIST guidance is voluntary, the guidelines provide valuable insights and best practices to protect network systems and data.

70. NIST guidance includes recommendations for risk assessments, risk management strategies, system access controls, training, data security, network monitoring, breach detection, and mitigation of existing anomalies.

71. Defendants' failure to protect massive amounts of Payment Information throughout the multi-month breach period belies any assertion that Defendants employed proper data security protocols or adhered to the spirit of the NIST guidance.

DEFENDANTS' SECURITY OBLIGATIONS

72. Defendants breached their obligations to Plaintiffs and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems and data. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect customers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to sufficiently train its employees in the proper handling of emails containing PII;

e. Failing to fully comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act, and;

f. Failing to adhere to industry standards for cybersecurity.

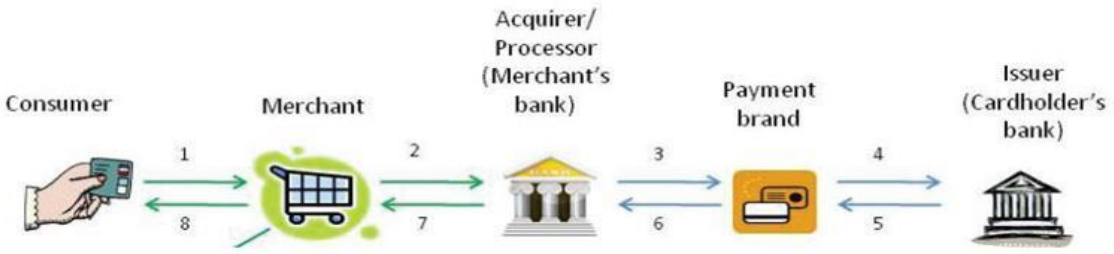
73. As the result of computer systems in need of security upgrading, inadequate procedures for handling emails containing viruses or other malignant computer code, and employees who opened files containing the virus or malignant code that perpetrated the cyberattack, Defendants negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information.

74. Accordingly, as outlined below, Plaintiffs' and Class Members' daily lives were severely disrupted. What's more, they now face an increased risk of fraud and identity theft. Plaintiffs and the Class Members also lost the benefit of the bargain they made with Defendants.

DATA BREACHES, FRAUD AND IDENTITY THEFT

75. In a debit or credit card purchase transaction, card data must flow through multiple systems and parties to be processed. Generally, the cardholder presents a credit or debit card to an e-commerce retailer (through an e-commerce website) to pay for merchandise. The card is then "swiped" and information about the card and the purchase is stored in the retailer's computers and then transmitted to the acquirer or processor (i.e., the retailer's bank). The acquirer relays the transaction information to the payment card company, who then sends the information to the issuer (i.e., cardholder's bank). The issuer then notifies the payment card company of its decision to authorize or reject the transaction. See graphic below:[6]

[6] Source: "Payments 101: Credit and Debit Card Payments," a white paper by First Data, at: https://www.firstdata.com/downloads/thought-leadership/payments101wp.pdf (last accessed October 27, 2020).



1	The consumer selects a card for payment. The cardholder data is entered into the merchant's payment system, which could be the point-of-sale (POS) terminal/software or an e-commerce website.
2	The card data is sent to an acquirer/payment processor, whose job it is to route the data through the payments system for processing. With e-commerce transactions, a "gateway" provider may provide the link from the merchant's website to the acquirer.
3	The acquirer/processor sends the data to the payment brand (e.g. Visa, MasterCard, American Express, etc.) who forward it to the issuing bank/issusing bank processor
4	The issuing bank/processor verifies that the card is legitimate, not reported lost or stolen, and that the account has the appropriate amount of credit/funds available to pay for the transaction.
5	If so, the issuer generates an authorization number and routes this number back to the card brand. With the authorization, the issuing bank agrees to fund the purchase on the consumer's behalf.
6	The card brand forwards the authorization code back to the acquirer/processor.
7	The acquirer/processor sends the authorization code back to the merchant.
8	The merchant concludes the sale with the customer.

76. There are two points in the payment process where sensitive cardholder data is at risk of being exposed or stolen: pre-authorization when the merchant has captured a consumer's data and it is waiting to be sent to the acquirer; and post-authorization when cardholder data has been sent back to the merchant with the authorization response from the acquirer, and it is placed into some form of storage in the merchant's servers.

77. Encryption mitigates security weaknesses that exist when cardholder data has been stored, but not yet authorized, by using algorithmic schemes to transform plain text information into a non-readable format called "ciphertext." By scrambling the payment card data the moment it is "swiped," hackers who steal the data are left with useless, unreadable text in the place of payment card numbers accompanying the cardholder's personal information stored in the retailer's computers.

78. However, when the data is not encrypted, hackers can target what they refer to as the *fullz*–a term used by criminals to refer to stealing the full primary account number, card holder

contact information, credit card number, CVC code, and expiration date. The *fullz* is exactly what appears to have been scraped from Defendants' ecommerce platform. Typically, these hackers insert virtual credit card skimmers or scrapers (also known as *formjacking*) into a web application (usually the shopping cart) and proceed to scrape credit card information to sell on the dark web.[7]

79. At the very least, Defendants chose not to invest in the technology to encrypt payment card data at point-of-sale to make its customers' data more secure; failed to install updates, patches, and malware protection or to install them in a timely manner to protect against a data security breach; and/or failed to provide sufficient control employee credentials and access to computer systems to prevent a security breach and/or theft of payment card data.

80. The FTC hosted a workshop to discuss "informational injuries" which are injuries that consumers suffer from privacy and security incidents, such as data breaches or unauthorized disclosure of data.[8] Exposure of personal information that a consumer wishes to keep private may cause both market and non-market harm to the consumer, such as the ability to obtain or keep employment and negative impact on consumer's relationships with family, friends and coworkers. Consumers loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

81. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, or take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more

---

[7] *Magecart Hits 80 Major eCommerce Sites in Card-Skimming Bonanza*, Threatpost, Aug. 28, 2019, *available at*: https://threatpost.com/magecart-ecommerce-card-skimming-bonanza/147765/, last visited on May 24, 2021.

[8] *FTC Information Injury Workshop, BE and BCP Staff Perspective,* Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf.

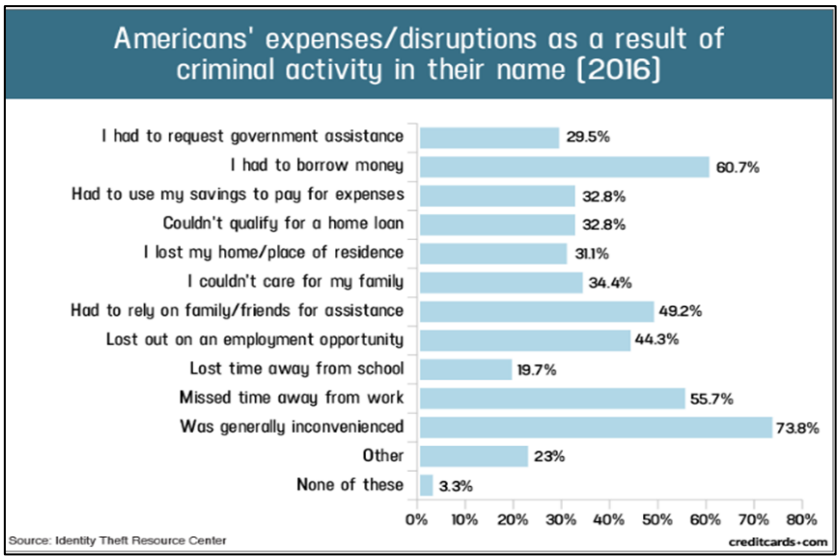
accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

82. The detailed information obtained in the instant data breach regarding the nature of the purchases Plaintiffs and Class Members made on the ShopRuger.com website makes the risk of phishing attacks even greater. With detailed purchase information, criminals will be able to reference those specific purchases that Plaintiffs and Class Members will recognize, making it harder for Plaintiffs and Class Members to identify such phishing attacks.

83. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[9]

[9] *See IdentityTheft.gov*, Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited August 11, 2022).

84. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of PII:[10]



85. Moreover, theft of Private Information is also gravely serious. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

86. As noted, the fact that this data breach included information regarding firearm related purchases makes the information obtained uniquely valuable to criminals looking to steal a gun.

87. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[11]

---

[10] Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), *available at* https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/.

[11] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/270/262904.html.

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

88. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

89. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiffs and Class Members must vigilantly monitor their financial accounts for many years to come.

PLAINTIFFS AND CLASS MEMBERS' DAMAGES

90. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

91. Plaintiffs' Private Information, including their sensitive PII, was compromised as a direct and proximate result of the Data Breach.

92. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud, identity theft, and burglary regarding their firearms.

93. As a direct and proximate result of Ruger's conduct, Plaintiffs and Class Members have been forced to expend time dealing with the effects of the Data Breach.

94. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as fraudulent transactions billed in their names, loans opened in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

95. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential

fraudsters could use that information to target such schemes more effectively to Plaintiffs and Class Members.

96. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, along with costs to secure their firearms from theft, or other similar costs directly or indirectly related to the Data Breach.

97. The information that Defendants maintain regarding Plaintiffs and Class Members, when combined with publicly available information, would allow nefarious actors to paint a complete financial and personal history of Plaintiffs and Class Members.

98. Plaintiffs and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiffs and Class Members overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiffs and Class Members paid, to Ruger was intended to be used by Defendants to fund adequate security of Defendants' computer property and protect Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and the Class Members did not get what they paid for.

99. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts and records for misuse.

100. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled;

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come, and;

l. Securing their homes and firearms against the increased risk of burglary.

101. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendants, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

102. As a direct and proximate result of Defendants' actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and either have suffered harm or are at an imminent and increased risk of future harm.

CLASS ALLEGATIONS

103. Plaintiffs bring this action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of themselves and on behalf of all other persons similarly situated (the "Class").

104. Plaintiffs proposes the following Class definitions, subject to amendment as appropriate:

> **Nationwide Class**
> All individuals in the United States who had Private Information stolen as a result of the Data Breach, including all who were sent a notice of the Data Breach.
>
> **Texas Subclass**
> All residents of Texas who had Private Information stolen as a result of the Data Breach, including all who were sent a notice of the Data Breach.
>
> **Michigan Subclass**
> All residents of Michigan who had Private Information stolen as a result of the Data Breach, including all who were sent a notice of the Data Breach.

105. Excluded from each of the above Classes are Defendants and their parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded are any Judge to whom this case is assigned as well as his or her judicial staff and immediate family members.

106. Plaintiffs reserve the right to modify or amend the definitions of the proposed Classes before the Court determines whether certification is appropriate.

107. Each of the proposed classes meet the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

108. Numerosity**.** The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of thousands of customers of Ruger whose data

was compromised in the Data Breach. The identities of Class Members are ascertainable through Defendants' records, Class Members' records, publication notice, self-identification, and other means.

109. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendants engaged in the conduct alleged herein;
b. Whether Ruger's conduct violated the Michigan Consumer Protection Act, invoked below;
c. When Defendants actually learned of the data breach and whether its response was adequate;
d. Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;
e. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
f. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
g. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;
h. Whether Defendants owed a duty to Class Members to safeguard their Private Information;
i. Whether Defendants breached their duty to Class Members to safeguard their Private Information;
j. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

k. Whether Defendants had a legal duty to provide timely and accurate notice of the data breach to Plaintiffs and the Class Members;

l. Whether Defendants breached their duty to provide timely and accurate notice of the data breach to Plaintiffs and the Class Members;

m. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;

n. What damages Plaintiffs and Class Members suffered as a result of Defendants' misconduct;

o. Whether Defendants' conduct was negligent;

p. Whether Defendants' conduct was *per se* negligent;

q. Whether Defendants were unjustly enriched;

r. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages;

s. Whether Plaintiffs and the other Class Members are entitled to additional credit or identity monitoring and are entitled to other monetary relief; and

t. Whether Plaintiffs and the Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

110. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach.

111. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

112. Predominance**.** Defendants have engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising

from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

113. Superiority**.** A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

114. Class certification also is appropriate under Fed. R. Civ. P. 23(b)(2). Ruger has acted or has refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

115. Finally, all members of the proposed Class are readily ascertainable. Defendants have access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Ruger.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR ALTERNATIVELY THE STATE SUBCLASSES)

116. Plaintiffs restate and reallege all proceeding allegations above and hereafter as if fully set forth herein.

117. Defendants knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in

safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

118. Defendants knew, or should have known, of the risks inherent in collecting the Private Information of Plaintiffs and the Class Members and the importance of adequate security.

119. Defendants owed a duty of care to Plaintiffs and the Class Members whose Private Information was entrusted to them. Defendants' duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private Information in their possession;

b. To protect customers' Private Information using reasonable and adequate security procedures and systems that are compliant with the industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in their possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class Members pursuant to the Connecticut law (where Ruger is headquartered), specifically C.G.S.A. § 36a-701b;

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches, and

f. To promptly notify Plaintiffs and the Class Members of the data breach, and to disclose precisely the type(s) of information compromise.

120. Plaintiffs and the Class Members were foreseeable and probable victims of any inadequate security practices, and Defendants owed them a duty of care not to subject them to an unreasonable risk of harm.

121. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiffs and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within Defendants' possession.

122. Defendants, by their actions and/or omissions, breached their duty of care by failing to provide, or by acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and the Class Members.

123. Defendants, by their actions and/or omissions, breached their duty of care by failing to promptly identify the Data Breach and then provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

124. Defendants acted with reckless disregard for the rights of Plaintiffs and the Class Members by failing to provide prompt and adequate individual notice of the data breach so that they could take measures to protect themselves from damages caused by the fraudulent use the Private Information compromised in the data breach.

125. Defendants had a special relationship with Plaintiffs and the Class Members. Plaintiffs' and the Class Members' willingness to entrust Defendants with their Private Information was predicated on the understanding that Ruger would take adequate security precautions. Moreover, only Defendants had the ability to protect their systems (and the Private Information that it stored on them) from attack.

126. Defendants' breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information to be compromised.

127. Defendants' breaches of duty caused a foreseeable risk of harm to Plaintiffs and Class Members to suffer from identity theft, loss of time and money to monitor their finances for fraud, loss of control over their Private Information, and increased risk of burglary or theft of their firearms.

128. As a result of Defendants' negligence and breach of duties, Plaintiffs and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, and will be used for fraudulent purposes.

129. Defendants also had independent duties under state laws that required it to reasonably safeguard Plaintiffs' and the Class Members' Private Information and promptly notify them about the data breach.

130. But for Defendants' wrongful and negligent breach of the duties it owed Plaintiffs and the Class Members, their Private Information either would not have been compromised or they would have been able to prevent some or all their damages.

131. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and the Class Members have suffered damages and are at imminent risk of further harm.

132. The injury and harm that Plaintiffs and the Class Members suffered (as alleged above) was reasonably foreseeable.

133. The injury and harm that Plaintiffs and the Class Members suffered (as alleged above) was the direct and proximate result of Defendants' negligent conduct.

134. Plaintiffs and the Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

135. In addition to monetary relief, Plaintiffs and the Class Members also are entitled to injunctive relief requiring Defendants to, *inter alia*, strengthen their data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and the Class Members.

COUNT II
NEGLIGENCE *PER SE*
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR ALTERNATIVELY THE STATE SUBCLASSES)

136. Plaintiffs restate and reallege the allegations in paragraphs 1-115 as if fully set forth herein.

137. Pursuant to Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, Ruger had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information, including PII, of Plaintiffs and the Class Members.

138. Plaintiffs and the Class Members are within the class of persons that the FTCA is intended to protect.

139. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect Private Information. The FTC publications described above, and the industry standard data and cybersecurity measures, also form part of the basis of Ruger's duty in this regard.

140. Defendants violated the FTCA by failing to use reasonable measures to protect Private Information of Plaintiffs and the Class and not complying with applicable industry standards, as described herein.

141. Defendants' violations of the FTCA constitutes negligence *per se*.

142. In connection with its consumer transactions, Defendants engaged in unfair, abusive or deceptive acts, omissions or practices by, misrepresenting material facts to Plaintiffs and the Class, in connection with providing utility services, by representing that Defendants did and would comply with the requirements of relevant federal and state law pertaining to the privacy and security of Plaintiffs and the Class Members' Private Information, such requirements included, but are not limited to, those imposed by laws such as the FTCA.

143. It was reasonably foreseeable that the failure to reasonably protect and secure Plaintiffs' and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to Defendants' servers, networks, databases, and/or computers that stored or contained Plaintiffs' and Class Members' Private Information.

144. Plaintiffs' and Class Members' Private Information constitutes personal property that was stolen due to Defendants' negligence, resulting in harm, injury and damages to Plaintiffs and Class Members.

145. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including PII, as a result of the data breach including but not

limited to damages from lost time and effort to mitigate the actual and potential impact of the data breach on their lives.

146. Defendants breached their duties to Plaintiffs and the Class under these laws by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and the Class Members' Private Information.

147. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and the Class Members, Plaintiffs and the Class Members would not have been injured.

148. The injury and harm suffered by Plaintiffs and the Class Members was the reasonably foreseeable result of Defendants' breach of its duties. Defendants knew or should have known that they were failing to meet their duties, and that Defendants' breach would cause Plaintiffs and the Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

149. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, injuries damages arising from their inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the data breach and/or false or fraudulent charges stemming from the data breach, including but not limited to late fees charges; damages from lost time and effort to mitigate the actual and potential impact of the data breach on their lives including, *inter alia*, by contacting their financial institutions to place to dispute fraudulent charges, closing or modifying financial accounts, closely reviewing and monitoring their accounts for unauthorized activity.

150. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and the Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

151. In addition to monetary relief, Plaintiffs and the Class Members also are entitled to injunctive relief requiring Defendants to, *inter alia*, strengthen their data security systems and

monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and the Class Members.

COUNT III
BREACH OF CONTRACT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR ALTERNATIVELY THE STATE SUBCLASSES)

152. Plaintiffs restate and reallege the allegations in paragraphs 1-115 as if fully set forth herein.

153. Plaintiffs and Class Members entered into a valid and enforceable contract when they paid money to Defendants in exchange for services, which included promises to secure, safeguard, protect, keep private, and not disclose Plaintiffs' and Class Members' Private Information.

154. Ruger's Privacy Policy memorialized the rights and obligations of Ruger and its customers. This document was provided to Plaintiffs in a manner and during a time where it became part of the agreement for services. This Privacy Policy is applicable to Freestyle as well.

155. In the Privacy Notice, Ruger commits to protecting the privacy and security of private information and promises to never share customer information unless given written permission or if state or federal law requires it.

156. Ruger further states in the Privacy Notice that it is required by law to maintain the privacy and security of PII and promises not to use or share PII other than as described in the Privacy Notice.

157. Plaintiffs and the Class Members fully performed their obligations under their contracts with Ruger.

158. Ruger, and Freestyle, acting on Ruger's behalf, did not secure, safeguard, protect, and/or keep private Plaintiff' and Class Members' PII and/or it disclosed their PII to third parties, and therefore Ruger breached its contract with Plaintiffs and Class Members.

159. Defendants allowed third parties to access, copy, and/or transfer Plaintiffs' and Class Members' PII, without permission, and therefore Ruger breached its contracts with Plaintiffs and Class Members.

160. Defendants' failure to satisfy their confidentiality and privacy obligations resulted in Ruger providing services to Plaintiffs and Class Members that were of a diminished value.

161. As a result, Plaintiffs and Class Members have been harmed, damaged, and/or injured as described herein.

162. In addition to monetary relief, Plaintiffs and the Class Members also are entitled to injunctive relief requiring Defendants to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and the Class Members.

COUNT IV
BREACH OF IMPLIED CONTRACT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR ALTERNATIVELY THE STATE SUBCLASSES)

163. Plaintiffs restate and reallege the allegations in paragraphs 1-115 as if fully set forth herein.

164. Ruger provides ecommerce services to Plaintiffs and Class Members. Plaintiffs and Class Members also formed an implied contract with Defendants regarding the provision of those services through their collective conduct, including by Plaintiffs and Class Members paying for services and/or receiving goods from Defendants.

165. Through Defendants' performance of, sale of, and/or purchase of goods and services, they knew or should have known that they must protect Plaintiffs' and Class Members' confidential Personal Information in accordance with Defendants' policies, practices, and applicable law.

166. As consideration, Plaintiffs and Class Members paid money to Ruger for goods and turned over valuable Personal Information to Defendants. Accordingly, Plaintiffs and Class Members bargained with Defendants to securely maintain and store their Personal Information.

167. Defendants violated these contracts by failing to employ reasonable and adequate security measures to secure Plaintiffs' and Class Members' Personal Information and by disclosing it for purposes not required or permitted under the contracts or agreements.

168. Plaintiffs and Class Members have been damaged by Defendants' conduct, including by paying for data and cybersecurity protection that they did not receive, as well as by incurring the harms and injuries arising from the Data Breach now and in the future.

COUNT V
VIOLATION OF TEXAS DECEPTIVE TRADE PRACTICES ACT
TEXAS BUS. & COM. CODE §§ 17.41, *ET SEQ*.
(ON BEHALF OF THE TEXAS SUBCLASS)

169. Plaintiff Woods restates and realleges the allegations in paragraphs 1-115 as if fully set forth herein.

170. As fully alleged above, Defendants engaged in unfair and deceptive acts and practices in violation of Texas Deceptive Trade Practices Act (Texas Bus. & Com. Code §§ 17.41, *et seq*.).

171. Defendants are "persons," as defined by Tex. Bus. & Com. Code § 17.45(3).

172. Plaintiff Woods and the Texas Subclass members are "consumers," as defined by Tex. Bus. & Com. Code § 17.45(4).

173. Defendants advertised, offered, or sold goods or services in Texas and engaged in trade or commerce directly or indirectly affecting the people of Texas, as defined by Tex. Bus. & Com. Code § 17.45(6).

174. Defendants engaged in false, misleading, or deceptive acts and practices, in violation of Tex. Bus. & Com. Code § 17.46(b), including:

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have;

b. Representing that goods or services are of a particular standard, quality or grade, if they are of another; and

c. Advertising goods or services with intent not to sell them as advertised.

175. Defendants' false, misleading, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Woods and Texas Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Woods and Texas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Texas's data security statute, Tex. Bus. & Com. Code § 521.052, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Woods and Texas Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Woods and Texas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Texas's data security statute, Tex. Bus. & Com. Code § 521.052;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff Woods and Texas Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Woods and Texas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Texas's data security statute, Tex. Bus. & Com. Code § 521.052.

176. Defendants intended to mislead Plaintiff Woods and Texas Subclass members and induce them to rely on their misrepresentations and omissions.

177. Reasonable individuals would be misled by Defendants' misrepresentations and/or omissions concerning the security of their Private Information, because they assume companies that collect PII from customers will properly safeguard that Personal Information in a manner consistent with industry standards and practices.

178. Had Plaintiff Woods and Texas Subclass members known of Defendants' failure to maintain adequate security measures to protect their Personal Information, Plaintiff Woods and Texas Subclass members would not have entrusted their Personal Information to Defendants.

179. Plaintiff Woods and Texas Subclass Members were injured because: a) they would not have paid for goods from Ruger had they known the true nature and character of Defendants' data security practices; b) Plaintiff Woods and Texas Subclass Members would not have entrusted their Private Information to Defendants in the absence of promises that Defendants would keep their information reasonably secure, and c) Plaintiff Woods and Texas Subclass Members would not have entrusted their Private Information to Defendants in the absence of the promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

180. As a result, Plaintiff Woods and Texas Subclass Members have been damaged in an amount to be proven at trial.

181. On behalf of Plaintiff Woods and Texas Subclass, Plaintiff Woods seeks to enjoin the unlawful acts and practices described herein, to recover his actual damages, three times actual damages, and reasonable attorneys' fees.

COUNT VI
MICHIGAN CONSUMER PROTECTION ACT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR ALTERNATIVELY THE STATE SUBCLASSES)

182. Plaintiff Copeland restates and realleges the allegations in paragraphs 1-115 as if fully set forth herein.

183. Defendants, Plaintiff Copeland, and Michigan Subclass members are "persons" as defined by Mich. Comp. Laws Ann. § 445.903(d).

184. Defendants advertised, offered, or sold goods or services in Michigan and engaged in trade or commerce directly or indirectly affecting the people of Michigan, as defined by Mich. Comp. Laws Ann. § 445.903(g).

185. Defendants engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Mich. Comp. Laws Ann. § 445.903(1), including:

a. Representing that their goods and services have characteristics, uses, and benefits that they do not have, in violation of Mich. Comp. Laws Ann. § 445.903(1)(c);
b. Representing that their goods and services are of a particular standard or quality if they are of another in violation of Mich. Comp. Laws Ann. § 445.903(1)(e);
c. Making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is, in violation of Mich. Comp. Laws Ann. § 445.903(1)(bb); and
d. Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive matter, in violation of Mich. Comp. Laws Ann. § 445.903(1)(cc).

186. Defendants' unfair, unconscionable, and deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Copeland and Michigan Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Copeland and Michigan Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Copeland and Michigan Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Copeland and Michigan Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff Copeland and Michigan Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Copeland and Michigan Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

187. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Personal Information.

188. Defendants intended to mislead Plaintiff Copeland and Michigan Subclass members and induce them to rely on their misrepresentations and omissions.

189. Defendants acted intentionally, knowingly, and maliciously to violate Michigan's Consumer Protection Act, and recklessly disregarded Plaintiff Copeland and Michigan Subclass members' rights.

190. As a direct and proximate result of Defendants' unfair, unconscionable, and deceptive practices, Plaintiff Copeland and Michigan Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; securing their firearms; an increased, imminent risk of fraud, identity theft and burglary; along with loss of value of their Personal Information.

191. Plaintiff Copeland and Michigan Subclass members seek all monetary and nonmonetary relief allowed by law, including the greater of actual damages or $250, injunctive relief, and any other relief that is just and proper

COUNT VII
UNJUST ENRICHMENT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR ALTERNATIVELY THE STATE SUBCLASSES)

192. Plaintiffs restate and reallege the allegations in paragraphs 1-115 as if fully set forth herein.

193. This count is plead in the alternative to Count III above.

194. Defendants have retained the benefits of their unlawful conduct including the amounts received for data and cybersecurity practices that they did not provide. Due to

Defendants' conduct alleged herein, it would be unjust and inequitable under the circumstances for Defendants to be permitted to retain the benefit of their wrongful conduct.

195. Plaintiffs and Class Members are entitled to full refunds, restitution and/or damages from Defendants and/or an order of this Court proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from their wrongful conduct. If necessary, the establishment of a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation may be created.

196. Additionally, Plaintiffs and the Class Members may not have an adequate remedy at law against Defendants, and accordingly plead this claim for unjust enrichment in addition to or, in the alternative to, other claims pleaded herein.

197. Plaintiffs and members of the Nationwide class conferred a benefit on Defendants by paying for data and cybersecurity procedures to protect their Private Information that they did not receive.

COUNT VIII
DECLARATORY JUDGMENT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR ALTERNATIVELY THE STATE SUBCLASS)

198. Plaintiffs restate and reallege the allegations in paragraphs 1-115 as if fully set forth herein.

199. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

200. Defendants owe a duty of care to Plaintiffs and the Class Members which required it to adequately secure Private Information.

201. Defendants still possess Private Information regarding Plaintiffs and the Class Members.

202. Plaintiffs allege that Defendants' data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their Private Information, and remain at imminent risk that further compromises of their Private Information will occur in the future.

203. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owe a legal duty to secure customers' Private Information and to timely notify customers of a data breach under the common law and Section 5 of the FTCA;

b. Defendants' existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect customers' Private Information; and

c. Defendants continue to breach this legal duty by failing to employ reasonable measures to secure customers' Private Information.

204. This Court also should issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with law and industry standards to protect customers' Private Information, including the following:

a. Order Defendants to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and the Class Members.

b. Order Defendants to comply with their explicit or implicit contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a

periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training their security personnel regarding any new or modified procedures;

iv. segmenting their user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendants' systems;

v. conducting regular database scanning and securing checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

vii. meaningfully educating their users about the threats they face as a result of the loss of their Private Information to third parties, as well as the steps Defendants' customers must take to protect themselves.

205. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendants. The risk of another such breach is real, immediate, and substantial. If another breach at Defendants occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

206. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

207. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at Defendants, thus eliminating the additional injuries that would result to Plaintiffs and customers whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Classes described above, seek the following relief:

c. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the classes as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are a proper representatives of the Classes requested herein;

d. Judgment in favor of Plaintiffs and the Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

e. An order providing injunctive and other equitable relief as necessary to protect the interests of the Classes as requested herein;

f. An order instructing Defendants to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiffs and the Class Members;

g. An order requiring Defendants to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

h. A judgment in favor of Plaintiffs and the Classes awarding them pre-judgment and post judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law, and

i. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demands a trial by jury on all triable issues.

DATED: October 27, 2022

Respectfully submitted,

/s/ Thomas Stavola, Jr.

Thomas Stavola, Jr.
SIRI & GLIMSTAD LLP
Mason A. Barney (*pro hac vice* to be filed)
Sean Nation (*pro hac vice* to be filed)
745 Fifth Ave, Suite 500
New York, NY 10151
Tel: (212) 532-1091
E: mbarney@sirillp.com
E: snation@sirillp.com